AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

§ 8.11 Records.

(a) The records of an advisory committee consist of all papers and documents which are prepared for or by and/or made available to the committee, and are maintained by the office responsible for the committee. Such records are *inter alia* agenda, drafts, minutes, notices, press releases, reports, studies, transcripts, and working papers.

(b) The Advisory Committee Management Officer maintains the Department's official records relating to the management of all committees.

§ 8.12 Financial records.

Accurate records will be kept by the responsible committee office of all operating and salary costs of a committee. (See instruction item 17 on SF–248.)

§ 8.13 Availability of records.

The records of a committee are to be made available upon request in accordance with the Department's regulations promulgated in accordance with the provisions of the Freedom of Information Act (40 FEDERAL REGISTER 7256–7529, February 19, 1975).

§ 8.14 Public inquiries.

Public inquiries concerning the implementation of the Federal Advisory Committee Act and the management of the advisory committees of the Department should be addressed to the Advisory Committee Management Officer, Management Systems Staff, Department of State, Washington, DC 20520.

PART 9—SECURITY INFORMATION REGULATIONS

Sec.

AUTHORITY: E.O. 12958 (60 FR 19825, April 20, 1995) as amended; Information Security Oversight Office Directive No. 1, 32 CFR 2001 (68 FR 55168, Sept. 22, 2003).

SOURCE: 72 FR 30972, June 5, 2007, unless otherwise noted.

§ 9.1 Basis.

These regulations, taken together with the Information Security Oversight Office Directive No. 1 dated September 22, 2003, and Volume 5 of the Department's Foreign Affairs Manual, provide the basis for the security classification program of the U.S. Department of State (''the Department'') implementing Executive Order 12958, ''Classified National Security Information'', as amended (''the Executive Order'').

§ 9.2 Objective.

The objective of the Department's classification program is to ensure that national security information is protected from unauthorized disclosure, but only to the extent and for such a period as is necessary.

§ 9.3 Senior agency official.

The Executive Order requires that each agency that originates or handles classified information designate a senior agency official to direct and administer its information security program. The Department's senior agency official is the Under Secretary of State for Management. The senior agency official is assisted in carrying out the provisions of the Executive Order and the Department's information security program by the Assistant Secretary for Diplomatic Security, the Assistant Secretary for Administration, and the Deputy Assistant Secretary for Information Sharing Services.

§ 9.4 Original classification.

(a) *Definition.* Original classification is the initial determination that certain information requires protection against unauthorized disclosure in the interest of national security (*i.e.*, national defense or foreign relations of the United States), together with a designation of the level of classification.

(b) *Classification levels.* (1) *Top Secret* shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) *Secret* shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) *Confidential* shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(c) *Classification requirements and limitations.* (1) Information may not be considered for classification unless it concerns:

(i) Military plans, weapons systems, or operations;

(ii) Foreign government information;

(iii) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(iv) Foreign relations or foreign activities of the United States, including confidential sources;

(v) Scientific, technological, or economic matters relating to the national security; which includes defense against transnational terrorism;

(vi) United States Government programs for safeguarding nuclear materials or facilities;

(vii) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(viii) Weapons of mass destruction.

(2) In classifying information, the public's interest in access to government information must be balanced against the need to protect national security information.

(3) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, or agency, to restrain competition, or to prevent or delay the release of information that does not require protection in the interest of the national security.

(4) A reference to classified documents that does not directly or indirectly disclose classified information may not be classified or used as a basis for classification.

(5) Only information owned by, produced by or for, or under the control of the U.S. Government may be classified.

(6) The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

(d) *Duration of classification.* (1) Information shall be classified for as long as is required by national security considerations, subject to the limitations set forth in section 1.5 of the Executive Order. When it can be determined, a specific date or event for declassification in less than 10 years shall be set by the original classification authority at the time the information is originally classified. If a specific date or event for declassification cannot be determined, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years.

(2) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under the Executive Order are met.

(3) Information marked for an indefinite duration of classification under predecessor orders, such as ''Originating Agency's Determination Required'' (OADR) or containing no declassification instructions shall be subject to the declassification provisions of Part 3 of the Order, including the provisions of section 3.3 regarding automatic declassification of records older than 25 years.

§ 9.5 Original classification authority.

(a) Authority for original classification of information as *Top Secret* may be exercised by the Secretary and those officials delegated this authority in

writing by the Secretary. Such authority has been delegated to the Deputy Secretary, the Under Secretaries, Assistant Secretaries and other Executive Level IV officials and their deputies; Chiefs of Mission, Charge d'Affaires, and Principal Officers at autonomous posts abroad; and to other officers within the Department as set forth in Department Notice dated May 26, 2000.

(b) Authority for original classification of information as *Secret or Confidential* may be exercised only by the Secretary, the Senior Agency Official, and those officials delegated this authority in writing by the Secretary or the Senior Agency Official. Such authority has been delegated to Office Directors and Division Chiefs in the Department, Section Heads in Embassies and Consulates abroad, and other officers within the Department as set forth in Department Notice dated May 26, 2000. In the absence of the Secret or Confidential classification authority, the person designated to act for that official may exercise that authority.

§ 9.6 Derivative classification.

(a) *Definition*. Derivative classification is the incorporating, paraphrasing, restating or generating in new form information that is already classified and the marking of the new material consistent with the classification of the source material. Duplication or reproduction of existing classified information is not derivative classification.

(b) *Responsibility*. Information classified derivatively from other classified information shall be classified and marked in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide and shall comply with the standards set forth in sections 2.1–2.2 of the Executive Order and the ISOO implementing directives in 32 CFR 2001.22.

(c) *Department of State Classification Guide*. The Department of State Classification Guide (DSCG) is the primary authority for the classification of information in documents created by Department of State personnel. The Guide is classified ''Confidential'' and is found on the Department of State's classified Web site.

§ 9.7 Identification and marking.

(a) Classified information shall be marked pursuant to the standards set forth in section 1.6 of the Executive Order; ISOO implementing directives in 32 CFR 2001, Subpart B; and internal Department guidance in 12 Foreign Affairs Manual (FAM).

(b) Foreign government information shall retain its original classification markings or be marked and classified at a U.S. classification level that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(c) Information assigned a level of classification under predecessor executive orders shall be considered as classified at that level of classification.

§ 9.8 Classification challenges.

(a) *Challenges*. Holders of information pertaining to the Department of State who believe that its classification status is improper are expected and encouraged to challenge the classification status of the information. Holders of information making challenges to the classification status of information shall not be subject to retribution for such action. Informal, usually oral, challenges are encouraged. Formal challenges to classification actions shall be in writing to an original classification authority (OCA) with jurisdiction over the information and a copy of the challenge shall be sent to the Office of Information Programs and Services (IPS) of the Department of State, SA–2, 515 22nd St. NW., Washington, DC 20522–6001. The Department (either the OCA or IPS) shall provide an initial response in writing within 60 days.

(b) *Appeal procedures and time limits*. A negative response may be appealed to the Department's Appeals Review Panel (ARP) and should be sent to: Chairman, Appeals Review Panel, c/o Information and Privacy Coordinator/Appeals Officer, at the IPS address given above. The appeal shall include a

copy of the original challenge, the response, and any additional information the appellant believes would assist the ARP in reaching its decision. The ARP shall respond within 90 days of receipt of the appeal. A negative decision by the ARP may be appealed to the Interagency Security Classification Appeals Panel (ISCAP) referenced in section 5.3 of Executive Order 12958. If the Department fails to respond to a formal challenge within 120 days or if the ARP fails to respond to an appeal within 90 days, the challenge may be sent to the ISCAP.

§ 9.9 Declassification and downgrading.

(a) *Declassification processes.* Declassification of classified information may occur:

(1) After review of material in response to a Freedom of Information Act (FOIA) request, mandatory declassification review request, discovery request, subpoena, classification challenge, or other information access or declassification request;

(2) After review as part of the Department's systematic declassification review program;

(3) As a result of the elapse of the time or the occurrence of the event specified at the time of classification;

(4) By operation of the automatic declassification provisions of section 3.3 of the Executive Order with respect to material more than 25 years old.

(b) *Downgrading.* When material classified at the Top Secret level is reviewed for declassification and it is determined that classification continues to be warranted, a determination shall be made whether downgrading to a lower level of classification is appropriate. If downgrading is determined to be warranted, the classification level of the material shall be changed to the appropriate lower level.

(c) *Authority to downgrade and declassify.* (1) Classified information may be downgraded or declassified by the official who originally classified the information if that official is still serving in the same position, by a successor in that capacity, by a supervisory official of either, or by any other official specifically designated by the Secretary or the senior agency official.

(2) The Department shall maintain a record of Department officials specifically designated as declassification and downgrading authorities.

(d) *Declassification in the public interest.* Although information that continues to meet the classification criteria of the Executive Order or a predecessor order normally requires continued protection, in some exceptional cases the need to protect information may be outweighed by the public interest in disclosure of the information. When such a question arises, it shall be referred to the Secretary or the Senior Agency Official for decision on whether, as an exercise of discretion, the information should be declassified and disclosed. This provision does not amplify or modify the substantive criteria or procedures for classification or create any substantive or procedural right subject to judicial review.

(e) *Public dissemination of declassified information.* Declassification of information is not authorization for its public disclosure. Previously classified information that is declassified may be subject to withholding from public disclosure under the FOIA, the Privacy Act, and various statutory confidentiality provisions.

§ 9.10 Mandatory declassification review.

All requests to the Department by a member of the public, a government employee, or an agency to declassify and release information shall result in a prompt declassification review of the information in accordance with procedures set forth in 22 CFR 171.20–25. Mandatory declassification review requests should be directed to the Information and Privacy Coordinator, U.S. Department of State, SA–2, 515 22nd St., NW., Washington, DC 20522–6001.

§ 9.11 Systematic declassification review.

The Information and Privacy Coordinator shall be responsible for conducting a program for systematic declassification review of historically valuable records that were exempted from the automatic declassification provisions of section 3.3 of the Executive Order. The Information and Privacy Coordinator shall prioritize such

review on the basis of researcher interest and the likelihood of declassification upon review.

§ 9.12 Access to classified information by historical researchers and certain former government personnel.

For Department procedures regarding the access to classified information by historical researchers and certain former government personnel, see Sec. 171.24 of this Title.

§ 9.13 Safeguarding.

Specific controls on the use, processing, storage, reproduction, and transmittal of classified information within the Department to provide protection for such information and to prevent access by unauthorized persons are contained in Volume 12 of the Department's Foreign Affairs Manual.

PART 9a—SECURITY INFORMATION REGULATIONS APPLICABLE TO CERTAIN INTERNATIONAL ENERGY PROGRAMS; RELATED MATERIAL

Sec.

AUTHORITY: E.O. 11932 (41 FR 32691), E.O. 11652 (37 FR 5209, National Security Council Directive of May 17, 1972 (37 FR 10053).

SOURCE: 42 FR 46516, Sept. 16, 1977; 42 FR 57687, Nov. 4, 1977, unless otherwise noted.

§ 9a.1 Security of certain information and material related to the International Energy Program.

These regulations implement Executive Order 11932 dated August 4, 1976 (41 FR 32691, August 5, 1976) entitled ''Classification of Certain Information and Material Obtained from Advisory Bodies Created to Implement the International Energy Program.''

§ 9a.2 General policy.

(a) The United States has entered into the Agreement on an International Energy Program of November 18, 1974, which created the International Energy Agency (IEA). This program is a substantial factor in the conduct of our foreign relations and an important element of our national security. The effectiveness of the Agreement depends significantly upon the provision and exchange of information and material by participants in advisory bodies created by the IEA. Confidentiality is essential to assure the free and open discussion necessary to accomplish the tasks assigned to those bodies.

(b) These regulations establish procedures for the classification, declassification, storage, access, and dissemination of certain information related to the International Energy Program.

§ 9a.3 Scope.

These regulations apply to all information and material classified by the United States under the provisions of E.O. 11932, dated August 4, 1976 entitled ''Classification of Certain Information and Material Obtained From Advisory Bodies Created To Implement The International Energy Program.''

§ 9a.4 Classification.

(a) Section 1 of E.O. 11932, August 4, 1976 directs that information and material obtained pursuant to the International Energy Program and which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States shall be classified pursuant to Executive Order 11652.

(b) Information and material, including transcripts, records, and communications, in the possession of the United States Government which has been obtained pursuant to (1) section 252(c)(3), (d)(2) or (e)(3) of the Energy Policy and Conservation Act (89 Stat. 871, 42 U.S.C. 6272(c)(3), (d)(2), (e)(3)), or (2) The Voluntary Agreement and Program Relating to the International Energy Program (40 FR 16041, April 8, 1975), or (3) the Voluntary Agreement and Plan of Action to Implement the International Energy Program (41 FR 13998, April 1, 1976), or (4) Any similar